

BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-009753

(43)Date of publication of application : 11.01.2002

(51)Int.Cl.

H04L 9/08
G06F 12/14
G09C 1/00
G11B 20/10

(21)Application number : 2000-186174

(22)Date of filing : 21.06.2000

(71)Applicant : SONY CORP

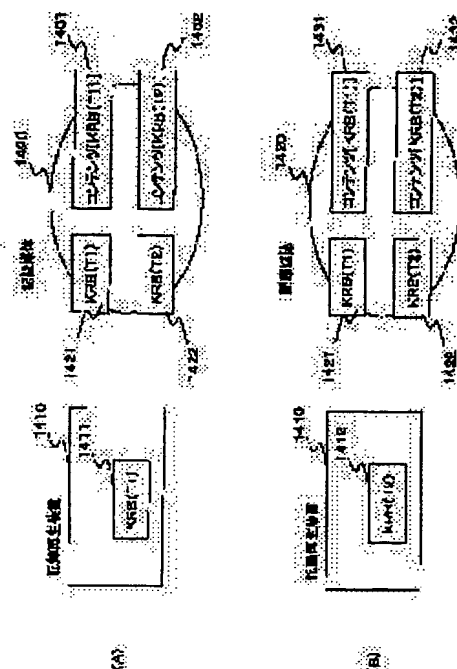
(72)Inventor : ASANO TOMOYUKI
OSAWA YOSHITOMO
ISHIGURO RYUJI
MITSUZAWA ATSUSHI
OISHI TAKEO

(54) INFORMATION RECORDING DEVICE, INFORMATION REPRODUCING DEVICE, INFORMATION RECORDING METHOD, INFORMATION REPRODUCING METHOD, AND INFORMATION RECORDING MEDIUM, AND PROGRAM PROVIDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information recording and reproducing device and its method that selectively use a key revision block(KRB) of the newest version so as to encrypt contents and store them to a recording medium.

SOLUTION: The method is configured to store KRBs having different generations and versions to a recording medium. In the case of detecting the newest KRB, it is stored in a memory in the recording and reproducing device. In the contents storage processing to the recording medium, newest available KRBs are detected among KRBs in the memory of the recording and reproducing device and KRBs on the recording medium to acquire an encryption processing key such as a media key and to execute encryption processing for the contents. Thus, it is possible to store encrypted contents on the basis of a KRB of a newer version to the recording medium at all times.



LEGAL STATUS

[Date of request for examination]

26.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998,2003 Japan Patent Office

(10) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-9753

(P2002-9753A)

(43) 公開日 平成14年1月11日 (2002.1.11)

(51) Int.Cl.	識別記号	FI	キーワード(参考)
H04L 9/08		G06F 12/14	320B 5B017
G06F 12/14	320	G09C 1/00	660D 5D044
G09C 1/00	660	G11B 20/10	H 5J104
G11B 20/10		H04L 9/00	601B

審査請求 未請求 請求項の数20 O L (全 31 頁)

(21) 出願番号 特願2000-186174(P2000-186174)

(22) 出願日 平成12年6月21日 (2000.6.21)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 大澤 健知

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

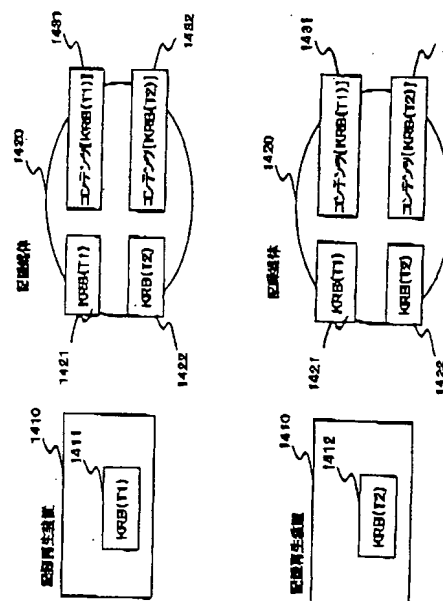
最終頁に続く

(54) 【発明の名称】 情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体

(57) 【要約】

【課題】 最新バージョンのキー更新ブロック (KRB) を選択的に使用してコンテンツを暗号化して記録媒体に格納する情報記録再生装置および方法を提供する。

【解決手段】 複数の異なる世代、バージョンを持つ KRB を記録媒体に格納する構成とした。さらに、最新の KRB を検出した場合は、記録再生装置内のメモリに格納する。記録媒体へのコンテンツ格納処理においては、記録再生装置のメモリ内の KRB、記録媒体上の複数の KRB 中から、利用可能な最新 KRB を検出して暗号処理用キー、例えばメディアキーを取得して、コンテンツの暗号処理を実行する。従って、常により新しいバージョンの KRB に基づく暗号化コンテンツを記録媒体に格納することが可能となる。



(A)

(B)

(2)

特開2002-9759

1

【特許請求の範囲】

【請求項1】記録媒体に情報を記録する情報記録装置において、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーを格納し、前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロック

(KRB)を格納するメモリ手段と、

前記情報記録装置に内蔵した前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロック(KRB)の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、を有し、

前記暗号処理手段は、

前記記録媒体に対するコンテンツの暗号化および格納処理において、記録媒体に格納されたキー更新ブロック

(KRB)、および情報記録装置自身のメモリに格納したキー更新ブロック(KRB)の中から利用可能な最新のキー更新ブロック(KRB)を検出して、検出した利用可能な最新のキー更新ブロック(KRB)の復号処理によって得られる暗号処理用キーを用いて記録媒体に対する格納データの暗号化処理を実行する構成を有することを特徴とする情報記録装置。

【請求項2】前記暗号処理用キーは、複数の情報記録装置に共通なマスターキー、情報記録装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする請求項1に記載の情報記録装置。

【請求項3】前記情報記録装置は、さらに、記録媒体に格納されたキー更新ブロック(KRB)、および情報記録装置自身の有するキー更新ブロック(KRB)中の利用可能な最新のキー更新ブロック(KRB)が、情報記録装置自身のメモリに格納したキー更新ブロック(KRB)であり、該最新のキー更新ブロック(KRB)が記録媒体に未格納である場合において、記録媒体に対する前記最新のキー更新ブロック(KRB)の書き込み処理を実行する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項4】前記情報記録装置は、さらに、記録媒体に格納されたキー更新ブロック(KRB)、および情報記録装置自身の有するキー更新ブロック(KRB)中の利用可能な最新のキー更新ブロック(KRB)が、記録媒体に格納したキー更新ブロック(KRB)であり、該最新のキー更新ブロック(KRB)が情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロック(KRB)の書き込み処理を実行する構成を有するこ

2

とを特徴とする請求項1に記載の情報記録装置。

【請求項5】前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を暗号処理用キー提供対象リーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、

キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項6】前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求項1に記載の情報記録装置。

【請求項7】記録媒体から情報を再生する情報再生装置において、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーを格納し、前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロック

(KRB)を格納するメモリ手段と、

前記情報再生装置に内蔵した前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロック(KRB)の復号処理を実行して、前記記録媒体に格納された暗号データの復号処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に格納された暗号データの復号処理を実行する暗号処理手段と、を有し、

前記暗号処理手段は、

前記記録媒体に格納された暗号データの復号処理において、記録媒体に格納されたキー更新ブロック(KRB)、および情報再生装置自身のメモリに格納したキー更新ブロック(KRB)の中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック(KRB)を検出して、検出したキー更新ブロック(KRB)の復号処理によって得られる暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行する構成を有することを特徴とする情報再生装置。

【請求項8】前記暗号処理用キーは、複数の情報再生装置に共通なマスターキー、情報再生装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする請求項7に記載の情報再生装置。

【請求項9】前記情報再生装置は、さらに、

記録媒体に格納されたキー更新ブロック(KRB)、お

(3)

特開2002-9759

3

4

よび情報再生装置自身の有するキー更新ブロック (KRB) 中の利用可能な最新のキー更新ブロック (KRB) が、記録媒体に格納したキー更新ブロック (KRB) であり、該最新のキー更新ブロック (KRB) が情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロック (KRB) の書き込み処理を実行する構成を有することを特徴とする請求項7に記載の情報再生装置。

【請求項10】前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック (KRB) を暗号処理用キー提供対象リーフの情報再生装置に配布する構成であり、前記情報再生装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、

キー更新ブロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする請求項7に記載の情報再生装置。

【請求項11】前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求項7に記載の情報再生装置。

【請求項12】複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録方法であり、

記録媒体に格納されたキー更新ブロック (KRB)、および情報記録装置自身のメモリに格納したキー更新ブロック (KRB) 中から利用可能な最新のキー更新ブロック (KRB) を検出するKRB検出ステップと、

前記KRB検出ステップにおいて、検出された利用可能な最新のキー更新ブロック (KRB) について、前記情報記録装置に内蔵したノードキーまたはリーフキーの少なくともいずれかを用いてキー更新ブロック (KRB) の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行するKRB復号処理ステップと、

前記KRB復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップと、を有することを特徴とする情報記録方法。

【請求項13】前記情報記録方法において、

前記KRB検出ステップにおいて、検出した利用可能な最新のキー更新ブロック (KRB) が、情報記録装置自身のメモリに格納したキー更新ブロック (KRB) であり、該最新のキー更新ブロック (KRB) が記録媒体に

未格納である場合において、記録媒体に対する前記最新のキー更新ブロック (KRB) の書き込み処理を実行することを特徴とする請求項12に記載の情報記録方法。

【請求項14】前記情報記録方法において、

前記KRB検出ステップにおいて、検出した利用可能な最新のキー更新ブロック (KRB) が、記録媒体に格納したキー更新ブロック (KRB) であり、該最新のキー更新ブロック (KRB) が情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロック (KRB) の書き込み処理を実行することを特徴とする請求項12に記載の情報記録方法。

【請求項15】複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生方法であり、

記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、

記録媒体に格納されたキー更新ブロック (KRB)、および情報再生装置自身のメモリに格納したキー更新ブロック (KRB) 中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック (KRB) を検出する検出ステップと、

前記検出ステップにおいて検出したキー更新ブロック (KRB) の復号処理によって暗号処理用キーを生成するステップと、

生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと、

を有することを特徴とする情報再生方法。

【請求項16】前記情報再生方法において、

前記KRB検出ステップにおいて、検出した利用可能な最新のキー更新ブロック (KRB) が、記録媒体に格納したキー更新ブロック (KRB) であり、該最新のキー更新ブロック (KRB) が情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロック (KRB) の書き込み処理を実行することを特徴とする請求項15に記載の情報再生方法。

【請求項17】情報を記録可能な情報記録媒体であって、

複数の異なる情報記録装置または情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録または再生装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック (KRB) を、異なる構成を持つ複数のキー更新ブロック (KRB) として、格納したことを特徴とする情報記録媒体。

【請求項18】前記複数のキー更新ブロック (KRB)

10

20

30

40

50

(4)

特開2002-9759

5

の各々は、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求項17に記載の情報記録媒体。

【請求項19】複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
記録媒体に格納されたキー更新ブロック（KRB）、および情報記録装置自身のメモリに格納したキー更新ブロック（KRB）の中から利用可能な最新のキー更新ブロック（KRB）を検出するKRB検出ステップと、
前記KRB検出ステップにおいて、検出された利用可能な最新のキー更新ブロック（KRB）について、前記情報記録装置に内蔵したノードキーまたはリーフキーの少なくともいずれかを用いてキー更新ブロック（KRB）の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行するKRB復号処理ステップと、
前記KRB復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップと、
を有することを特徴とするプログラム提供媒体。

【請求項20】複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、
記録媒体に格納されたキー更新ブロック（KRB）、および情報再生装置自身のメモリに格納したキー更新ブロック（KRB）の中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック（KRB）を検出する検出ステップと、
前記検出ステップにおいて検出したキー更新ブロック（KRB）の復号処理によって暗号処理用キーを生成するステップと、
生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと、
を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報

6

記録媒体、並びにプログラム提供媒体に関し、本構造の階層的鍵配信方式を用いてマスターキーあるいはメディアキー等の暗号鍵更新を行ない、さらに、記録媒体に新たに格納されるコンテンツに関して、より新しいキーを用いた暗号化を可能とした構成に関する。具体的には、各記録再生機器をn分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、コンテンツの記録、再生に必要な鍵を配信するとともに、複数の世代、バージョンの異なるキーを記録媒体に格納し、新たに格納するコンテンツに対する暗号化処理の際に、より新しいキーを検出して、これを用いて記録を行う構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【0002】

【従来の技術】デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【0003】例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインタフェース（DIF）から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【0004】具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、1度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー（copy free）となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可（copy once allowed）となっている場合には、SCMS信号をコピー禁止（copy p

(5)

特開 2002-9753

7

rohibited)に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止 (copy prohibited) となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【0005】しかしながら、SCMSは上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【0006】コンテンツ・スクランブルシステムでは、DVD-ROM(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー (復号鍵) が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

【0007】一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行えないことになり、不正コピーが防止されるようになっている。

【0008】しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体 (以下、適宜、ROMメディアという) を対象としており、ユーザによるデータの書き込みが可能な記録媒体 (以下、適宜、RAMメディアという) への適用については考慮されていない。

【0009】即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【0010】そこで、本出願人は、先の特許出願、特開

8

平11-224461号公報 (特願平10-25310号) において、個々の記録媒体を識別する為の情報 (以下、媒体識別情報と記述する) を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【0011】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー (マスターキー) により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製 (違法コピー) ができないように、その動作が規定される。

【0012】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【0013】

【発明が解決しようとする課題】ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、1つの機器で記録された媒体を他の機器で再生可能とする (インターオペラビリティを確保する) ために必要な条件であるからである。

【0014】しかし、この方式においては、攻撃者が1つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵 (デバイスキー) を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【0015】上記問題を解決する構成として、本出願人は、各情報記録再生装置をn分木の各葉 (リーフ) に配置した構成の鍵配信方法を用い、記録媒体もしくは通信

50

(8)

特開 2002-9759

9

10

回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキーもしくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願（特願平2000-105328）している。具体的には、記録媒体への記録もしくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えばn分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理した情報を含むキー更新ブロック

（KRB）を各情報記録再生装置に配信し、キー更新ブロック（KRB）を受信した各情報記録再生装置のKRB復号処理により、各装置が記録もしくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

【0016】上記構成は、特定のシステム（記録再生装置グループ）の中のある装置が攻撃者の攻撃を受けて、その秘密であるデバイスキーが露呈したことが発覚した場合、それ以降に製造する記録媒体においては、秘密が露呈した記録再生装置をシステムから排除する、すなわち、排除されていない装置との記録再生の互換性をとれなくすることができるという特徴を持つ。

【0017】しかし、この構成では、秘密が露呈した機器をシステムから排除できるのは、それが発覚した以降に製造される記録媒体においてのみであり、それ以前に製造された記録媒体においては、実際にデータを記録するのが上記の発覚時点以降だとしても、記録されたデータを、露呈した鍵で復号することができてしまう、すなわち、排除すべき装置を実際に排除できる場合が少ないという課題がある。

【0018】本発明は、上記課題を解決することを目的とするものであり、秘密が露呈したことが発覚した後、それ以前に製造された記録媒体でも、記録されたデータを露呈した鍵で復号できないようにすることを可能とし、より有効なコンテンツ暗号化を可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供するものである。より、具体的には、記録媒体ごとにただひとつのメディアキーを設定するのではなく、複数のメディアキーを設定できるようにした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【0019】

【課題を解決するための手段】本発明の第1の側面は、記録媒体に情報を記録する情報記録装置において、複数の異なる情報記録装置をリーフとした階層ツリー構造を

構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーを格納し、前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロック（KRB）を格納するメモリ手段と、前記情報記録装置に内蔵した前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロック（KRB）の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、を有し、前記暗号処理手段は、前記記録媒体に対するコンテンツの暗号化および格納処理において、記録媒体に格納されたキー更新ブロック（KRB）、および情報記録装置自身のメモリに格納したキー更新ブロック（KRB）の中から利用可能な最新のキー更新ブロック（KRB）を検出して、検出した利用可能な最新のキー更新ブロック（KRB）の復号処理によって得られる暗号処理用キーを用いて記録媒体に対する格納データの暗号化処理を実行する構成を有することを特徴とする情報記録装置にある。

【0020】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理用キーは、複数の情報記録装置に共通なマスターキー、情報記録装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする。

【0021】さらに、本発明の情報記録装置の一実施態様において、記録媒体に格納されたキー更新ブロック（KRB）、および情報記録装置自身の有するキー更新ブロック（KRB）中の利用可能な最新のキー更新ブロック（KRB）が、情報記録装置自身のメモリに格納したキー更新ブロック（KRB）であり、該最新のキー更新ブロック（KRB）が記録媒体に未格納である場合において、記録媒体に対する前記最新のキー更新ブロック（KRB）の書き込み処理を実行する構成を有することを特徴とする。

【0022】さらに、本発明の情報記録装置の一実施態様において、記録媒体に格納されたキー更新ブロック（KRB）、および情報記録装置自身の有するキー更新ブロック（KRB）中の利用可能な最新のキー更新ブロック（KRB）が、記録媒体に格納したキー更新ブロック（KRB）であり、該最新のキー更新ブロック（KRB）が情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロック（KRB）の書き込み処理を実行する構成を有することを特徴とする。

【0023】さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキーまたはリーフキーの少

(7)

特開2002-9753

11

なくともいずれかを含むキーにより暗号化したキー更新ブロック (KRB) を暗号処理用キー提供対象リーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、キー更新ブロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする。

【0024】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする。

【0025】さらに、本発明の第2の側面は、記録媒体から情報を再生する情報再生装置において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーを格納し、前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロック (KRB) を格納するメモリ手段と、前記情報再生装置に内蔵した前記ノードキーまたはリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロック (KRB) の復号処理を実行して、前記記録媒体に格納された暗号データの復号処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に格納された暗号データの復号処理を実行する暗号処理手段と、を有し、前記暗号処理手段は、前記記録媒体に格納された暗号データの復号処理において、記録媒体に格納されたキー更新ブロック (KRB)、および情報再生装置自身のメモリに格納したキー更新ブロック (KRB) 中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック (KRB) を検出して、検出したキー更新ブロック (KRB) の復号処理によって得られる暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行する構成を有することを特徴とする情報再生装置にある。

【0026】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理用キーは、複数の情報再生装置に共通なマスターキー、情報再生装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする。

【0027】さらに、本発明の情報再生装置の一実施態様において、記録媒体に格納されたキー更新ブロック (KRB)、および情報再生装置自身の有するキー更新ブロック (KRB) 中の利用可能な最新のキー更新ブロック (KRB) が、記録媒体に格納したキー更新ブロック (KRB) であり、該最新のキー更新ブロック (KRB) が情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新の

12

キー更新ブロック (KRB) の書き込み処理を実行する構成を有することを特徴とする。

【0028】さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック (KRB) を暗号処理用キー提供対象リーフの情報再生装置に配布する構成であり、前記情報再生装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、キー更新ブロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする。

【0029】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする。

【0030】さらに、本発明の第3の側面は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録方法であり、記録媒体に格納されたキー更新ブロック (KRB)、および情報記録装置自身のメモリに格納したキー更新ブロック (KRB) 中から利用可能な最新のキー更新ブロック (KRB) を検出するKRB検出ステップと、前記KRB検出ステップにおいて、検出された利用可能な最新のキー更新ブロック (KRB) について、前記情報記録装置に内蔵したノードキーまたはリーフキーの少なくともいずれかを用いてキー更新ブロック (KRB) の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行するKRB復号処理ステップと、前記KRB復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップと、を有することを特徴とする情報記録方法にある。

【0031】さらに、本発明の情報記録方法の一実施態様において、前記KRB検出ステップにおいて、検出した利用可能な最新のキー更新ブロック (KRB) が、情報記録装置自身のメモリに格納したキー更新ブロック (KRB) であり、該最新のキー更新ブロック (KRB) が記録媒体に未格納である場合において、記録媒体に対する前記最新のキー更新ブロック (KRB) の書き込み処理を実行することを特徴とする。

【0032】さらに、本発明の情報記録方法の一実施態様において、前記KRB検出ステップにおいて、検出した利用可能な最新のキー更新ブロック (KRB) が、記

(B)

特開2002-9753

13

録媒体に格納したキー更新ブロック (KRB) であり、該最新のキー更新ブロック (KRB) が情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロック (KRB) の書き込み処理を実行することを特徴とする。

【0033】さらに、本発明の第4の側面は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生方法であり、記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、記録媒体に格納されたキー更新ブロック (KRB)、および情報再生装置自身のメモリに格納したキー更新ブロック (KRB) から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック (KRB) を検出する検出ステップと、前記検出ステップにおいて検出したキー更新ブロック (KRB) の復号処理によって暗号処理用キーを生成するステップと、生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと、を有することを特徴とする情報再生方法にある。

【0034】さらに、本発明の情報再生方法の一実施態様において、前記KRB検出ステップにおいて、検出した利用可能な最新のキー更新ブロック (KRB) が、記録媒体に格納したキー更新ブロック (KRB) であり、該最新のキー更新ブロック (KRB) が情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロック (KRB) の書き込み処理を実行することを特徴とする。

【0035】さらに、本発明の第5の側面は、情報を記録可能な情報記録媒体であって、複数の異なる情報記録装置または情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録または再生装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック (KRB) を、異なる構成を持つ複数のキー更新ブロック (KRB) として、格納したことを特徴とする情報記録媒体にある。

【0036】さらに、本発明の情報記録媒体の一実施態様において、前記複数のキー更新ブロック (KRB) の各々は、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする。

【0037】さらに、本発明の第6の側面は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラ

14

ムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納されたキー更新ブロック (KRB)、および情報記録装置自身のメモリに格納したキー更新ブロック (KRB) から利用可能な最新のキー更新ブロック (KRB) を検出するKRB検出ステップと、前記KRB検出ステップにおいて、検出された利用可能な最新のキー更新ブロック (KRB) について、前記情報記録装置に内蔵したノードキーまたはリーフキーの少なくともいずれかを用いてキー更新ブロック (KRB) の復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行するKRB復号処理ステップと、前記KRB復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップと、を有することを特徴とするプログラム提供媒体にある。

【0038】さらに、本発明の第7の側面は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、記録媒体に格納されたキー更新ブロック (KRB)、および情報再生装置自身のメモリに格納したキー更新ブロック (KRB) から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック (KRB) を検出する検出ステップと、前記検出ステップにおいて検出したキー更新ブロック (KRB) の復号処理によって暗号処理用キーを生成するステップと、生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと、を有することを特徴とするプログラム提供媒体にある。

【0039】

【作用】本発明の構成においては、ツリー (木) 構造の階層的鍵配信方式を用いることにより、キー更新に必要な配信メッセージ量を小さく抑えている。すなわち、各機器をn分木の各葉 (リーフ) に配置した構成の鍵配信方式を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵 (マスターキーもしくはメディアキー) を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う。

【0040】また、本発明では、前述の問題を解決するために、記録媒体ごとにただひとつのメディアキーを設定するのではなく、複数のメディアキーを設定できるようにする。すなわち、記録媒体が製造されて市場に出ま

わった後も、より新しいメディアキーを算出するためのキー更新ブロック (KRB: Key Renewal Block) を記録再生装置が記録媒体に書きこめるようにする。データを記録媒体に記録する際には、記録再生装置は、記録媒体上のキー更新ブロック (KRB: Key Renewal Block) と、自身が格納するKRBのうち最新のものをを用いてメディアキーを算出してデータの暗号化に使用し、またその最新のKRBが記録媒体上ではなく自身が格納しているものであれば、それを記録媒体に格納するようにする。

【0041】さらに記録再生装置は、記録媒体にアクセスする際に記録媒体上の全KRBのバージョンを調べ、その中の最新のものが、自身が格納するものより新しければ、これを用いて自身が格納するKRBを最新のものに更新する。これらの処理によって、記録再生装置にはどんどん新しいKRBが格納され、またデータが記録される際には、その時点で記録再生装置と記録媒体が格納する最新のKRBにより算出されるメディアキーを用いてデータが暗号化されて記録されるから、たとえ記録媒体が製造されたのがとても古く、あらかじめ記録媒体に格納されているKRBが古いものであったとしても、データが記録される際には新しいKRBが使われる可能性が高いので、そのデータの安全性をより高く守ることが可能となる。

【0042】なお、本発明の第6、第7の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0043】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0044】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0045】

【発明の実施の形態】 【システム構成】 図1は、本発明を適用した記録再生装置100の一実施例構成を示すブロック図である。記録再生装置100は、入出力I/F (Interface) 120、MPEG (Moving Picture Experts Group) コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F (Interface) 140、暗号

処理手段150、ROM (Read Only Memory) 160、CPU (Central Processing Unit) 170、メモリ180、記録媒体195の記録媒体インタフェース (I/F) 190を有し、これらはバス110によって相互に接続されている。

【0046】入出力I/F 120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F 140に出力するとともに、入出力I/F 140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F 140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F 140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D (Analog Digital) 変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

【0047】暗号処理手段150は、例えば、1チップのLSI (Large Scale Integrated Circuit) で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0048】ROM 160は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。CPU 170は、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU 170が実行するプログラムや、CPU 170の動作に必要なデータを記憶する。記録媒体インタフェース190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し (再生し)、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。また、プログラムをROM 160に、デバイスキーをメモリ180に記憶する構成としてもよい。

【0049】記録媒体195は、例えば、DVD、CD

(10)

特開 2002-9753

17

等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

【0050】【データ記録処理およびデータ再生処理】次に、図1の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図2および図3のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体195に記録する場合においては、図2(A)のフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS201において、入出力I/F120は、供給されるデジタルコンテンツを受信し、バス110を介して、暗号処理手段150に出力する。

【0051】暗号処理手段150は、ステップS202において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス110を介して、記録媒体I/F190に出力する。暗号化コンテンツは、記録媒体I/F190を介して記録媒体195に記録(S203)され、記録処理を終了する。

【0052】なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを送送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む5社によって、5CDTCP(Five Company Digital Transmission Content Protection)（以下、適宜、DTCPという）が定められているが、このDTCPでは、コピーフリーでないデジタルコンテンツを装置相互間で送送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱うかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

【0053】このDTCPに規格に基づくデータ送受信においては、データ受信側の入出力I/F120は、ステップS201で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、DTCPに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段150に出力する。

【0054】DTCPによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その

18

暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

【0055】なお、DTCPによれば、正解には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、DTCPについては、例えば、<http://www.dtcp.com>のURL(Uniform Resource Locator)で特定されるWebページにおいて、インフォメーションバージョン(Informational Version)の取得が可能である。

【0056】次に、外部からのアナログ信号のコンテンツを、記録媒体195に記録する場合の処理について、図2(B)のフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力I/F140に供給されると、入出力I/F140は、ステップS221において、そのアナログコンテンツを受信し、ステップS222に進み、内蔵するA/D、D/Aコンバータ141でA/D変換して、デジタル信号のコンテンツ（デジタルコンテンツ）とする。

【0057】このデジタルコンテンツは、MPEGコーデック130に供給され、ステップS223において、MPEGエンコード、すなわちMPEG圧縮による符号化処理が実行され、バス110を介して、暗号処理手段150に供給される。

【0058】以下、ステップS224、S225において、図2(A)のステップS202、S203における処理と同様の処理が行われる。すなわち、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0059】次に、記録媒体195に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図3のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図3(A)のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップS301において、記録媒体I/F190によって、記録媒体195に記録された暗号化コンテンツが読み出され、バス110を介して、暗号処理手段150に出力される。

【0060】暗号処理手段150では、ステップS302において、記録媒体I/F190から供給される暗号

化コンテンツが復号処理され、復号データがバス110を介して、入出力I/F120に供給される。ステップS303において、入出力I/F120はデジタルコンテンツを、外部に出力し、再生処理を終了する。

【0061】なお、入出力I/F120は、ステップS303で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、DTCIPの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

【0062】記録媒体195に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図3(B)のフローチャートに従った再生処理が行われる。

【0063】即ち、ステップS321、S322において、図3(A)のステップS301、S302における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段150において得られた復号されたデジタルコンテンツは、バス110を介して、MPEGコーデック130に供給される。

【0064】MPEGコーデック130では、ステップS323において、デジタルコンテンツがMPEGデコード、すなわち伸長処理が実行され、入出力I/F140に供給される。入出力I/F140は、ステップS324において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換して、アナログコンテンツとする。そして、ステップS325に進み、入出力I/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【0065】【キー配布構成としてのツリー（木）構造について】次に、図1に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なキー、例えばメディアキーを、各機器に配布する構成について説明する。図4は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図4の最下段に示すナンバ0～15が個々の記録再生装置である。すなわち図4に示す木（ツリー）構造の各葉（リーフ：leaf）がそれぞれの記録再生装置に相当する。

【0066】各デバイス0～15は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーを自身で格納する。図4の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節（ノード）に記載されたキー：KR～K111をノードキーとする。

【0067】図4に示すツリー構成において、例えばデ

バイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図4のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0068】また、図4のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図4に示すキー配布構成が適用されている。

【0069】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図4の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図4の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図4のツリー中に複数存在する。

【0070】なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0071】このツリー構成において、図4から明らかのように、1つのグループに含まれる9つのデバイス0、1、2、3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0、1、2、3のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmaster

(12)

特開2002-9753

21

をノードキーK00で暗号化した値Enc(K00, Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kmaster)を解いてマスターキー: Kmasterを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0072】また、ある時点の世代: tにおいて、デバイス3の所有する鍵: K0011, K001, K00, K0, KRが攻撃者(ハッカー)により解析されて露呈したことが発覚した場合、それ以降、システム(デバイス0, 1, 2, 3のグループ)で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー: K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代(Generation): tの更新キーであることを示す。

【0073】更新キーの配布処理について説明する。キーの更新は、例えば、図5(A)に示すキー更新ブロック(KRB: Key Renewal Block)と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。

【0074】図5(A)に示すキー更新ブロック(KRB)には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図5の例は、図4に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図4から明らかなように、デバイス0, デバイス1は、更新ノードキーとしてK(t)00, K(t)0, K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK(t)001, K(t)00, K(t)0, K(t)Rが必要である。

【0075】図5(A)のKRBに示されるようにKRBには複数の暗号化キーが含まれる。最下段の暗号化キーは、Enc(K0010, K(t)001)である。これはデバイス2の持つリーフキーK0010によって暗号化された更新ノードキーK(t)001であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、K(t)001を得ることができる。また、復号により得たK(t)001を用いて、図5(A)の下から2段目の暗号化キーEnc(K(t)001, K(t)00)を復号可能となり、更新ノードキーK(t)00を得ることができる。以下順次、図5(A)の上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号し、更新ノードキーK(t)

22

0、図5(A)の上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号しK(t)Rを得る。一方、デバイス0, 1は、ノードキーK000は更新する対象に含まれておらず、更新ノードキーとして必要なのは、K(t)00, K(t)0, K(t)Rである。デバイス0, 1は、図5(A)の上から3段目の暗号化キーEnc(K000, K(t)00)を復号しK(t)00を取得し、以下、図5(A)の上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号し、更新ノードキーK(t)0、図5(A)の上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号しK(t)Rを得る。このようにして、デバイス0, 1, 2は更新した鍵K(t)Rを得ることができる。なお、図5(A)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0076】図4に示すツリー構造の上位段のノードキー: K(t)0, K(t)Rの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図5(B)のキー更新ブロック(KRB: Key Renewal Block)を用いることで、更新ノードキーK(t)00をデバイス0, 1, 2に配布することができる。

【0077】図5(B)に示すKRBは、例えば特定のグループの情報記録装置において共有する新たなマスターキー、情報記録装置固有のデバイスキー、あるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図4に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のマスターキーK(t)masterが必要であるとする。このとき、デバイス0, 1, 2, 3の共通のノードキーK00を更新したK(t)00を用いて新たな共通の更新マスターキー: K(t)masterを暗号化したデータEnc(K(t), K(t)master)を図5(B)に示すKRBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキーについても同様である。

【0078】すなわち、デバイス0, 1, 2はKRBを処理して得たK(t)00を用いて上記暗号文を復号すれば、t時点でのマスターキー: K(t)masterやメディアキー: K(t)mediaを得ることが可能になる。

【0079】以上をまとめると、各デバイスでの処理は、以下のように説明できる。

1. 各デバイスはそれぞれ、KRBのインデックス(index)部を見て、KRBで送られる木の構造を知る。
2. KRBによって更新されていない(生きている)ノードキーのうち最上位の鍵(この例では、デバイス0, 1ならK000、デバイス2ならK0010)を用いて暗号文を解くことによって、そのノードの親のノードの更新されたノードキーを得る。
3. 更新されたノードキーを用いて暗号文を解くことに

(13)

特開2002-9753

23

よって、そのノードの親のノードの更新されたノードキーを得る。

4. これを繰り返して、KRBの最上位のノードの更新されたノードキーを得る。

【0080】なお、KRBの世代 (Generation) は、そのKRBのバージョンを表し、たとえば新しいものは値を大きくしておくなど、その値を比較することによってKRBの新旧の比較が行えるようになっている。また、 $K(t)0$ 、 $K(t)R$ の更新が不要の場合には、図6

(B)のKRB (Key Renewal Block) を用いることで、 $K(t)00$ をデバイス0, 1, 2で共有することができる。すなわち、デバイス0, 1, 2, 3がある記録媒体を用いるひとつのグループを形成するとき、 $K(t)00$ を用いて伝送したメディアキーを用いて記録データを暗号化することにより、デバイス4など、その他のグループの機器からはアクセスされないデータとすることが可能となる。具体的に、たとえば図6(B)を用いてデバイス0, 1, 2は $K(t)00$ を共有するが、このKRBを格納した記録媒体に、 t 時点でのメディアキー $K(t)media$ を暗号化して格納しておく。デバイス0, 1, 2はKRBを処理して得た $K(t)00$ を用いて上記暗号文を復号し、 t 時点でのメディアキー $K(t)media$ を得る。

【0081】[KRBを使用したメディアキーの取得] 図6に、本出願人の先の特許出願である特願平2000-105328で提案した t 時点でのメディアキー $K(t)media$ を得る処理例として、 $K(t)00$ を用いて新たな共通のメディアキー $K(t)media$ を暗号化したデータ $Enc(K(t)00, K(t)media)$ と図6(B)に示すKRBとを記録媒体を介して受領したデバイス2の処理を示す。

【0082】図4に示すように、ある記録再生システムには、点線で囲まれた、デバイス0, 1, 2, 3の4つの装置が含まれるとする。図6は、デバイス3がリポートされたときに、記録媒体ごとに割り当てられるメディアキーを使用する場合に、記録再生装置 (デバイス2) が記録媒体上のコンテンツを暗号化もしくは復号するために必要なメディアキーを、記録媒体に格納されているKRB (Key Renewal Block) と記録再生装置が記憶するデバイスキーを用いて求める際の処理を表している。

【0083】デバイス2のメモリには、自分にのみ割り当てられたリーフキー K_{0010} と、それから木のルートまでの各ノード $001, 00, 0, R$ のノードキー (それぞれ、 $K_{001}, K_{00}, K_0, K_R$) が安全に格納されている。デバイス2は、図6の記録媒体に格納されているKRBのうち、インデックス (index) が 0010 の暗号文を自分の持つリーフキー K_{0010} で復号してノード 001 のノードキー $K(t)_{001}$ を計算し、次にそれを用いてインデックス (index) が 001 の暗号文を復号してノード 00 のノードキー K

24

(t) $_{00}$ を計算し、最後にそれを用いて暗号文を復号してメディアキー $K(t)_{media}$ を計算する。このようにして計算され、取得されたメディアキーを用いたデータの暗号化処理、復号処理態様について、以下、説明する。

【0084】[メディアキーを用いた暗号化処理、復号処理] 図7の処理ブロック図に従って、暗号処理手段150が実行するデータの暗号化処理および記録媒体に対する記録処理の一例について説明する。

【0085】記録再生装置700は自身の上述したKRBに基づく算出処理によってメディアキーを取得する。

【0086】次に、記録再生装置700は例えば光ディスクである記録媒体702に識別情報としてのディスクID (Disc ID) が既に記録されているかどうかを検査する。記録されていれば、ディスクID (Disc ID) を読み出し、記録されていなければ、暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクID (Disc ID) 1701を生成し、ディスクに記録する。ディスクID (Disc ID) はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【0087】記録再生装置700は、次にメディアキー701とディスクIDを用いて、ディスク固有キー (Disc Unique Key) を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法としては、図8に示すように、ブロック暗号関数を用いたハッシュ関数にメディアキーとディスクID (Disc ID) を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、メディアキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する例2の方法が適用できる。

【0088】次に、記録ごとの固有鍵であるタイトルキー (Title Key) を暗号処理手段150 (図1参照) においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成し、ディスク702に記録する。

【0089】次にディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイスID、あるいは、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス固有キー、いずれかの組合せから、タイトル固有キー (Title Unique Key) を生成する。

【0090】このタイトル固有キー (Title Unique Key) 生成の具体的な方法は、図9に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー (Title Key) とディスク固有キー (Disc Unique Key) と、デバイスID (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) を入力して得

られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、メディアキーとディスクID (Disc ID) とデバイスID (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー (Title Unique Key) として使用する例2の方法が適用できる。なお、再生機器制限とは、記録媒体に格納されたコンテンツデータを制限された特定の再生機器においてのみ再生可能とすることを意味する。

【0091】なお、上記の説明では、メディアキーとディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデバイスID、もしくはタイトルキー (Title Key) とデバイス固有キーからタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキーとディスクID (Disc ID) とタイトルキー (Title Key) と、デバイスIDもしくはデバイス固有キーから直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、メディアキー (Media Key) とディスクID (Disc ID) と、デバイスIDもしくはデバイス固有キーからタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0092】さらに、図7を用いて、その後の処理を説明する。被暗号化データとして入力されるブロックデータの先頭の第1〜4バイトが分離されて出力されるブロックシード (Block Seed) と、先に生成したタイトル固有キー (Title Unique Key) とから、そのブロックのデータを暗号化する鍵であるブロック・キー (Block Key) が生成される。

【0093】ブロック・キー (Block Key) の生成方法の例を図10に示す。図10では、いずれも32ビットのブロック・シード (Block Seed) と、64ビットのタイトル固有キー (Title Unique Key) とから、64ビットのブロックキー (Block Key) を生成する例を2つ示している。

【0094】上段に示す例1は、鍵長64ビット、入出力がそれぞれ64ビットの暗号関数を使用している。タイトル固有キー (Title Unique Key) をこの暗号関数の鍵とし、ブロックシード (Block Seed) と32ビットの定数 (コンスタント) を連結した値を入力して暗号化した結果をブロックキー (Block Key) としている。

【0095】例2は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー (Title Unique Key) とブロックシード (Block Seed) を連結した値をSHA-1に入力し、その160ビットの出力を、たとえば下位64ビットのみ使用するなど、64ビットに縮約

したものをブロックキー (Block Key) としている。

【0096】なお、上記ではディスク固有キー (Disc Unique Key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとにメディアキーとディスクID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) と、デバイスID、もしくはデバイス固有キーを用いてブロックキー (Block Key) を生成してもよい。

【0097】ブロックキーが生成されると、生成されたブロックキー (Block Key) を用いてブロックデータを暗号化する。図7の下段に示すように、ブロックシード (Block Seed) を含むブロックデータの先頭の第1〜mバイト (たとえばm=8バイト) は分離 (セレクト1608) されて暗号化対象とせず、m+1バイト目から最終データまでを暗号化する。なお、暗号化されないmバイト中にはブロック・シードとしての第1〜4バイトも含まれる。セレクトにより分離された第m+1バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化される。暗号化アルゴリズムとしては、たとえばFIPS46-2で規定されるDES (Data Encryption Standard) を用いることができる。

【0098】以上の処理により、コンテンツはブロック単位で、世代管理されたメディアキー、ブロック・シード等に基づいて生成されるブロックキーで暗号化が施されて記録媒体に格納される。

【0099】記録媒体に格納された暗号化コンテンツデータの復号および再生処理を説明するブロック図11に示す。

【0100】再生処理においては、図7〜図10を用いて説明した暗号化および記録処理と同様、メディアキーとディスクIDからディスク固有キーを生成し、ディスク固有キーと、タイトルキーからタイトル固有キーを生成し、さらにタイトルキーと記録媒体から読み取られるブロックシードとから、ブロックキーを生成して、ブロックキーを復号キーとして用い、記録媒体702から読み取られるブロック単位の暗号化データの復号処理を実行する。

【0101】上述のように、コンテンツデータの記録媒体に対する記録時の暗号化処理、および記録媒体からの再生時の復号処理においては、KRBに基づいてメディアキーを算出し、その後算出したメディアキーと他の識別子等に基づいて、コンテンツの暗号化処理用の鍵、または復号処理用の鍵を生成する。

【0102】なお、上述した例では、メディアキーを用いてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成を説明したが、メディアキー

(15)

特開 2002-9759

27

ではなく、複数の記録再生装置に共通のマスターキー、あるいは記録再生装置固有のデバイスキーをKRBから取得して、これらに基づいてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成としてもよい。さらに、KRBから取得されるメディアキー、マスターキー、あるいはデバイスキー自体をコンテンツデータの暗号化処理、および復号処理に用いるキーとして適用することも可能である。

【0103】上述のように、キー更新ブロック(KRB)を用いることにより、正当なライセンスを受けたデバイスに対してのみ安全に更新キーを提供し、提供したキーによって記録媒体に対するコンテンツ暗号化処理、または記録媒体から読み出したコンテンツの復号処理に用いるキーの生成が可能となる。上述の構成では、例えば1つの記録媒体にただ1つのキー更新ブロック(KRB)を格納し、これを利用して更新キーの取得を行なう例を説明したが、さらに、複数のキー更新ブロック(KRB)を格納した構成例について、以下説明する。この場合、後段で詳細に説明するが、記録媒体上の記録暗号化コンテンツデータの各々を、複数のキー更新ブロック(KRB)のいずれのKRBから生成されるメディアキーを用いて暗号化されたのが判別可能な情報を持つ構成とする。

【0104】また、記録媒体のみではなく、記録再生装置のメモリにKRBを格納する構成としてもよい。記録再生装置のキー更新ブロック(KRB)格納用の記憶手段は、書き換え可能な構成であり、記録再生装置は、記録媒体へのアクセス時、たとえば、記録媒体が記録再生装置に装着された際に、記録媒体上のKRBを検索し、その中で一番バージョンが新しいものが、自身が格納するものよりも新しければ、これを用いて自身の格納するKRBを更新する。

【0105】[KRBのフォーマット] 図12にキー更新ブロック(KRB: Key Renewal Block)のフォーマット例を示す。バージョン1201は、キー更新ブロック(KRB: Key Renewal Block)のバージョンを示す識別子である。デプスは、キー更新ブロック(KRB: Key Renewal Block)の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ1203は、キー更新ブロック(KRB: Key Renewal Block)中のデータ部の位置を示すポインタであり、タグポインタ1204はタグ部の位置、署名ポインタ1205は署名の位置を示すポインタである。データ部1206は、例えば更新するノードキーを暗号化したデータを格納する。

【0106】タグ部1207は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図13を用いて説明する。図13では、データとして先に図5(A)で説明したキー更新ブロック(KRB)を送付する例を示している。この時のデータは、図13の右の表に示すよう

28

になる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスはKRとなる。

【0107】暗号化キーの最上段のデータ $Enc(K(t)0, K(t)R)$ は、図13の左の階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは(左(L)タグ、右(R)タグ)として設定される。最上段のデータ $Enc(K(t)0, K(t)R)$ の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図13(c)に示すデータ列、およびタグ列が構成される。

【0108】図12に戻って、KRBフォーマットについてさらに説明する。署名(Signature)は、キー更新ブロック(KRB)を発行した例えばコンテンツ管理センタ、コンテンツプロバイダ、決済機関等が発行する電子署名である。KRBを受領したデバイスは署名検証によって正当なキー更新ブロック(KRB)発行者が発行したキー更新ブロック(KRB)であることを確認する。

【0109】[複数のキー更新ブロック(KRB)を選択利用する構成] 次に、記録媒体に複数のキー更新ブロック(KRB)を格納する構成、さらに、記録再生装置のメモリに最新のKRBを格納する処理、すなわち、記録再生装置側に格納したキー更新ブロック(KRB)を更新する処理について、図14のイメージ図および図15のフローチャートを用いて説明する。

【0110】図14の上段に示す(A)は、記録再生機器に記録媒体が装着される以前の状態で、記録再生装置1410に1つのキー更新ブロック(KRB)1411が格納され、記録媒体1420には、2つのキー更新ブロック(KRB)1421、1422が格納されている状態を示している。

【0111】記録再生装置1410に格納されたKRBは、バージョン(T1)のキー更新ブロック(KRB)1411であり、記録媒体1420に格納されたKRBは、バージョン(T1)のキー更新ブロック(KRB)1421、およびバージョン(T2)のキー更新ブロック(KRB)1422である。ここでバージョンT2はバージョンT1より新しいものとする。

【0112】また、記録媒体1420には、バージョン(T1)のキー更新ブロック(KRB)から生成されるメディアキーを用いて暗号化されたコンテンツ1431と、バージョン(T2)のキー更新ブロック(KRB)から生成されるメディアキーを用いて暗号化されたコンテンツ1432が格納されている。

【0113】記録媒体1420が記録再生装置1410

に装着された際、記録再生装置は図15のフローチャートに従って、自身の格納するキー更新ブロック(KRB)の更新処理を行う。

【0114】図15のステップS1501で、記録再生装置1410は、記録媒体1420に格納されているすべてのキー更新ブロック(KRB)の世代情報(Generation)であるバージョンを読出し、その中で最新のものを見つける。図14(A)に示す例では、バージョン(T2)のキー更新ブロック(KRB)1422が最新である。

【0115】ステップS1502において、記録再生装置1410は、記録再生装置内のメモリ(例えば図1のメモリ180)に格納しているキー更新ブロック(KRB)と、ステップS1501で検出した記録媒体1420上の最新KRB、すなわちバージョン(T2)のキー更新ブロック(KRB)1422との新旧を比較する。

【0116】この比較において、記録媒体上から検出したKRBの方が新しければステップS1503に進み、そうでなければステップS1503、S1504をスキップして処理を終了する。

【0117】図14(A)の例では、記録再生装置1410が格納しているのはバージョン(T1)のキー更新ブロック(KRB)1411であり、これよりバージョン(T2)のキー更新ブロック(KRB)1422の方が新しいので、ステップS1503に進む。

【0118】ステップS1503では、記録再生装置1410が保有しているリーフキー、ノードキーを用いて更新予定の最新のKRBが復号可能か否かを判定する。すなわち、先の図4、5、6等で説明したように、自己の有するリーフキー、あるいはノードキーによりキー更新ブロック(KRB)を順次復号し、世代の更新された世代情報：τの新バージョンのノードキー、例えばK(τ)00、あるいはルートキーK(τ)Rが取得可能か否かを判定する。この判定処理は、例えば図5に示すキー更新ブロック(KRB)において、いずれかのインデックスに自己の有するリーフキー、ノードキーをそのまま適用して復号可能な暗号化キーが格納されているか否かを判定することによって行なわれる。

【0119】ステップS1503において、記録再生装置1410が保有しているリーフキー、ノードキーを用いて更新予定の最新のKRBが復号可能であると判定された場合は、ステップS1504に進む。復号不可と判定された場合は、ステップS1504をスキップして処理を終了する。

【0120】ステップS1504では、ステップS1501で検出した記録媒体1420に格納された最新のKRBを用いて、記録再生装置1410がメモリに格納しているバージョン(T1)のキー更新ブロック(KRB)1411を更新する。この結果、図14(B)に示すように、記録再生装置1410に格納されるKRBが

バージョン(T2)のキー更新ブロック(KRB)1412に更新される。

【0121】次に、図16および図17のフローチャートを用いて、図1に示した記録再生装置が記録媒体にコンテンツデータを記録する処理を説明する。

【0122】図16の上段に示す(A)の記録再生装置1610は、バージョン(T2)のキー更新ブロック(KRB)1611を格納しており、コンテンツを暗号化して記録媒体1620に記録しようとしている。

【0123】記録媒体1620には、バージョン(T1)のキー更新ブロック(KRB)1621が記録されており、このキー更新ブロック(KRB)1621から生成されたメディアキーに基づいて暗号化されたコンテンツ1631が記録されている。

【0124】図17は、記録再生装置が記録媒体に対してコンテンツデータを記録する際の処理フローを示したものである。図17のフローの各ステップについて説明する。

【0125】ステップS1701において、記録再生装置1610は自身が格納するバージョン(T2)のキー更新ブロック(KRB)1611からメディアキーを生成する。

【0126】記録再生装置1610は、この記録媒体1620が装着されたときに、先に説明した図15のキー更新ブロック(KRB)更新処理を行っており、装置のメモリ内には装置および媒体上のキー更新ブロック(KRB)のうちの最新のもの、ここではバージョンT2のキー更新ブロック(KRB)が格納されている。

【0127】ステップS1702で、このメディアキーに基づいてコンテンツデータを暗号化する。この暗号化処理は、例えば先に図7を用いて説明した方法に従って実行される。その後、暗号化コンテンツデータは記録媒体1620に記録される。なお、暗号化コンテンツの記録媒体1620に対する格納処理の際に、そのコンテンツ暗号化に用いたメディアキーを取得したキー更新ブロック(KRB)の世代情報としてのバージョン、この場合は、キー更新ブロック(KRB)1611のバージョン(T2)を暗号化コンテンツに対応付けて記録媒体1620に記録する。この、キー更新ブロック(KRB)の世代情報としてのバージョン情報は、具体的にはたとえば、図7に示すタイトルキー等のコンテンツの付加情報と同様、コンテンツデータに関連づけられた管理ファイルとして構成されるデータ管理ファイル中に記録されて記録媒体1620に格納される。

【0128】次に、ステップS1703において、記録再生装置1610は、メディアキーを生成するのに用いたと同じバージョンのキー更新ブロック(KRB)が、記録媒体1620に格納されているかどうかを検査する。もし記録媒体1620に格納されていれば、ステップS1704をスキップして処理を終了し、格納され

ていなければ、S1704に進む。

【0129】ステップS1704では、記録再生装置1610は記録媒体1620に、メディアキーを生成するのに用いたのと同じバージョンのキー更新ブロック(KRB)、この場合は、バージョン(T2)のキー更新ブロック(KRB)を記録し、コンテンツデータの記録処理を終了する。以上の処理により、図16の(B)で示すように、記録媒体1620には、利用可能な最新のKRBから取得されるメディアキーを用いて暗号化した暗号化コンテンツデータと、およびコンテンツ暗号処理に必要となるメディアキーを得るために必要となる最新のキー更新ブロック(KRB)を記録媒体1620に記録することができる。

【0130】次に、上記のようにして、利用可能な最新のキー更新ブロック(KRB)に基づいて得られるキーを利用して暗号化され、記録されたコンテンツデータを、記録媒体から記録再生装置が読み出す処理を、図18のフローチャートを用いて説明する。

【0131】ステップS1801において、記録再生装置は、再生するコンテンツデータを暗号化したメディアキーを生成するキー更新ブロック(KRB)の世代情報としてのバージョンを読み出す。記録媒体上の各コンテンツデータに対応するキー更新ブロック(KRB)の世代情報としてのバージョンは、たとえば前述のデータ管理ファイルに書かれている。

【0132】ステップS1802で、記録再生装置は、記録媒体上に格納されている1以上のキー更新ブロック(KRB)のうち、ステップS1801において読み出した世代情報としてのバージョンと同一のバージョンを持つものを検出し、そのキー更新ブロック(KRB)を復号処理して、メディアキーを生成する。

【0133】次に、ステップS1803で、記録再生装置は、記録媒体からコンテンツデータを読み出し、S1802で生成したメディアキーに基づいてこれを復号して使用する。以上の処理により、記録媒体に格納されたコンテンツデータを再生することができる。

【0134】このように、本発明の情報記録再生装置では、複数の異なる世代、すなわちバージョンを持つキー更新ブロック(KRB)を格納した記録媒体から最新のキー更新ブロック(KRB)を取り出して、記録再生装置内のメモリに格納し、さらに、記録媒体に対するコンテンツ格納処理においては、記録再生装置内のメモリに格納されたKRB、および記録媒体に格納された複数のKRB中から、利用可能な最新のキー更新ブロック(KRB)を検出して、その最新KRBから暗号処理用のキー、例えばメディアキーを取得して、取得した最新のメディアキーを用いてコンテンツの暗号化処理を実行して、記録媒体に格納し、コンテンツの暗号化に用いたメディアキーを取得したキー更新ブロック(KRB)を新たに記録媒体に格納する構成とした。

【0135】このように複数のバージョンのKRBを記録媒体に格納可能とするとともに、異なるKRBから取得したメディアキーで暗号化したコンテンツを記録媒体に格納可能な構成とし、コンテンツを記録媒体に新たに記録する際には、その時点で記録再生装置と記録媒体が保有する最新のKRBに基づいて算出されるメディアキーを用いてコンテンツの暗号化がなされるので、例えば記録媒体の製造時にコンテンツ暗号化に用いられた古いバージョンのKRBが記録媒体に格納済みであっても、先に図4、図5を用いて説明したように、新たに経営管理センタ、プロバイダ、決済機関等が実行するキー更新処理によって発行された新しいバージョンのKRBを不正な機器をリボークして発行することにより、その後、記録媒体に格納される暗号化コンテンツは、正当な機器のみが取得可能な新しいバージョンのKRBから取得されるメディアキーに基づいて暗号化されることになるので、リボークされた機器における復号、再生を排除することが可能となる。

【0136】【記録処理におけるコピー制御】さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【0137】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの(コピー可能)かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【0138】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図1の記録再生装置の処理について、図19および図20のフローチャートを参照して説明する。

【0139】まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図19

(A)のフローチャートにしたがった記録処理が行われる。図19(A)の処理について説明する。図1の記録再生装置100を例として説明する。デジタル信号のコンテンツ(デジタルコンテンツ)が、例えば、IEEE1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS1901において、入出力I/F120は、そのデジタルコンテンツを受信し、ステップS1902に進む。

【0140】ステップS1902では、入出力I/F120は、受信したデジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力I/F120が受信したコンテンツが暗号化されていない場合(例えば、上述のDTCPを使用せずに、平文のコンテンツが、入出力I/F120に供給された場合)には、そのコンテンツは、コピー可能であると判定され

る。

【0141】また、記録再生装置100がDTCPに準拠している装置であるとし、DTCPに従って処理を実行するものとする。DTCPでは、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)が規定されている。EMIが00B (Bは、その前の値が2進数であることを表す) である場合は、コンテンツがコピーフリーのもの(Copy-free ly)であることを表し、EMIが01Bである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、EMIが10Bである場合は、コンテンツが、1度だけコピーして良いもの(Copy-one-generation)であることを表し、EMIが11Bである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

【0142】記録再生装置100の入出力I/F120に供給される信号にEMIが含まれ、そのEMIが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、EMIが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【0143】ステップS1902において、コンテンツがコピー可能でないと判定された場合、ステップS1903～S1904をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0144】また、ステップS1902において、コンテンツがコピー可能であると判定された場合、ステップS1903に進み、以下、ステップS1903～S1904において、図2(A)のステップS202、S203における処理と同様の処理が行われる。すなわち、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0145】なお、EMIは、入出力I/F120に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、EMI、あるいは、EMIと同様にコピー制御状態を表す情報(例えば、DTCPにおけるembedded CCIなど)も記録される。

【0146】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【0147】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図19(B)のフローチャートにしたがった記録処理が行われる。図19(B)の処理について説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS19

11において、そのアナログコンテンツを受信し、ステップS1912に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【0148】ここで、ステップS1912の判定処理は、例えば、入出力I/F140で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力I/F140で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【0149】また、例えば、CGMS-A信号は、デジタル信号のコピー制御に用いられるCGMS信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

【0150】従って、CGMS-A信号が、入出力I/F140で受信した信号に含まれ、かつ、そのCGMS-A信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【0151】さらに、例えば、マクロビジョン信号も、CGMS-A信号も、入出力I/F4で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【0152】ステップS1912において、アナログコンテンツがコピー可能でないと判定された場合、ステップS1913乃至S1916をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体195に記録されない。

【0153】また、ステップS1912において、アナログコンテンツがコピー可能であると判定された場合、ステップS1913に進み、以下、ステップS1913乃至S1916において、図2(B)のステップS222乃至S225における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、MPEG符号化、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【0154】なお、入出力I/F140で受信したアナログ信号に、CGMS-A信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのCGMS-A信号も、記録媒体に記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえ

ば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0155】【再生処理におけるコピー制御】次に、記録媒体に記録されたコンテンツを再生して、デジタルコンテンツとして外部に出力する場合においては、図20(A)のフローチャートにしたがった再生処理が行われる。図20(A)の処理について説明する。まず最初に、ステップS2001、S2002において、図3

(A)のステップS301、S302における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段150において復号処理がなされ、復号処理が実行されたデジタルコンテンツは、バス110を介して、入出力I/F120に供給される。

【0156】入出力I/F120は、ステップS2003において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI、あるいは、EMIと同様にコピー制御状態を表す情報(コピー制御情報)が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0157】また、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI等のコピー制御情報が含まれる場合、従って、コンテンツの記録時に、DTC Pの規格にしたがって、EMIが記録された場合には、そのEMI(記録されたEMI(Recorded EMI))が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。また、EMIが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないかと判定される。

【0158】なお、一般的には、記録されたEMIが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのEMIは記録時にNo-more-copiesに変換され、また、Copy-neverのEMIを持つデジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0159】ステップS2003において、コンテンツが、後でコピー可能なものであると判定された場合、ステップS2004に進み、入出力I/F120は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

【0160】また、ステップS2003において、コンテンツが、後でコピー可能なものでないかと判定された場合、ステップS2005に進み、入出力I/F120

は、例えば、DTC Pの規格等にしたがって、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0161】即ち、例えば、上述のように、記録されたEMIが、No-more-copiesである場合(もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMIがCopy-one-generationである場合)には、コンテンツは、それ以上のコピーは許されない。

【0162】このため、入出力I/F120は、DTC Pの規格にしたがって、相手の装置との間で認証を相互に行い、相手が正当な装置である場合(ここでは、DTC Pの規格に準拠した装置である場合)には、デジタルコンテンツを暗号化して、外部に出力する。

【0163】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図20(B)のフローチャートにしたがった再生処理が行われる。図20(B)の処理について説明する。ステップS2011乃至S2014において、図3(B)のステップS321乃至S324における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、MP EGデコード、D/A変換が実行される。これにより得られるアナログコンテンツは、入出力I/F140で受信される。

【0164】入出力I/F140は、ステップS2015において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、記録されていたコンテンツにEMI等のコピー制御情報いっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0165】また、コンテンツの記録時に、例えば、DTC Pの規格にしたがって、EMI等のコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【0166】また、EMI等のコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないかと判定される。

【0167】さらに、例えば、入出力I/F140に供給されるコンテンツにCGMS-A信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにCGMS-A信号が記録された場合には、そのC

(20)

特開 2002-9759

37

38

GMS-A信号が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものと判定される。また、CGMS-A信号が、Copy-neverであるときには、コンテンツは、後でコピー可能なものでない判定される。

【0168】ステップS2015において、コンテンツが、後でコピー可能であると判定された場合、ステップS2016に進み、入出力I/F140は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【0169】また、ステップS2015において、コンテンツが、後でコピー可能でないと判定された場合、ステップS2017に進み、入出力I/F140は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0170】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0171】このため、入出力I/F140は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すGMS-A信号を付加して、外部に出力する。また、例えば、記録されたCGMS-A信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力I/F140は、CGMS-A信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【0172】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【0173】〔データ処理手段の構成〕なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段150は暗号化／復号LSIとして構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図21は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【0174】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク2105やROM2109に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magnetooptical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体2110に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体2110は、いわゆるパッケージソフトウェアとして提供することができる。

【0175】なお、プログラムは、上述したようなリムーバブル記録媒体2110からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部2108で受信し、内蔵するハードディスク2105にインストールすることができる。

【0176】コンピュータは、CPU (Central Processing Unit) 2102を内蔵している。CPU2102には、バス2101を介して、入出力インタフェース2111が接続されており、CPU2102は、入出力インタフェース2110を介して、ユーザによって、キーボードやマウス等で構成される入力部2107が操作されることにより指令が入力されると、それにしたがって、ROM (Read Only Memory) 2103に格納されているプログラムを実行する。

【0177】あるいは、CPU2102は、ハードディスク2105に格納されているプログラム、衛星若しくはネットワークから転送され、通信部2108で受信されてハードディスク2105にインストールされたプログラム、またはドライブ2109に装着されたリムーバブル記録媒体2110から読み出されてハードディスク2105にインストールされたプログラムを、RAM (Random Access Memory) 2104にロードして実行する。

【0178】これにより、CPU2102は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU2102は、その処理結果を、必要に応じて、例えば、入出力インタフェース2111を介して、LCD (Liquid Crystal Display) やスピーカ等で構成される出力部2106から出力、あるいは、通信部2108から送信、さらには、ハードディスク2105に記録させる。

【0179】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あ

るいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0180】また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0181】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図1に示すCPU170が実行する1つのソフトウェアモジュールとして実現することも可能である。

【0182】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0183】

【発明の効果】以上、説明したように、本発明の情報記録再生装置によれば、複数の異なる世代、バージョンを持つキー更新ブロック（KRB）を記録媒体に格納可能とするとともに、最新のキー更新ブロック（KRB）を取り出して、記録再生装置内のメモリに格納することを可能とした。さらに、記録媒体に対するコンテンツ格納処理においては、記録再生装置内のメモリに格納されたKRB、および記録媒体に格納された複数のKRBの中から、利用可能な最新のキー更新ブロック（KRB）を検出して、その最新KRBから暗号処理用のキー、例えばメディアキーを取得して、取得した最新のメディアキーを用いてコンテンツの暗号化処理を実行して、記録媒体に格納し、コンテンツの暗号化に用いた例えばメディアキーを取得したキー更新ブロック（KRB）を新たに記録媒体に格納する構成とした。従って、コンテンツを記録媒体に新たに記録する際には、より新しいKRBに基づいて算出されるメディアキーを用いた暗号化がなされる。

【0184】従って、例えば記録媒体の製造時にコンテンツ暗号化に用いられた古いバージョンのKRBが記録媒体に格納済みであっても、より新しいKRBに基づく暗号処理キーによるコンテンツ暗号化および格納が可能となる。従って、キー更新処理によって新しいバージョンのKRBを不正な機器をリボークして発行することにより、その後は、正当な機器のみが取得可能な新しいバージョンのKRBから取得されるキーに基づく暗号化コンテンツを記録媒体に格納することが可能となるので、記録媒体自体の世代に関わらず、新規格納される暗号化コンテンツに関しては、リボークされた機器における利

用排除が可能となる。

【0185】また、本発明の情報記録再生装置によれば、記録再生装置にはほとんど新しいKRBが格納されることになり、またデータが記録される際には、その時点で記録再生装置と記録媒体が格納する最新のKRBにより算出されるメディアキーを用いてデータが暗号化されて記録されるから、たとえ記録媒体が製造されたのがとても古く、あらかじめ記録媒体に格納されているKRBが古いものであったとしても、データが記録される際には新しいKRBが使われ、暗号化コンテンツはより新しいバージョンの暗号処理キーで暗号化されることになる。このため、本発明によれば、映画や音楽などの著作権があるデータの不正な複製、例えば著作権者の意に反する複製が蔓延することを防ぐことができる。

【図面の簡単な説明】

【図1】本発明の情報記録再生装置の構成例を示すブロック図である。

【図2】本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図3】本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図4】本発明の情報記録再生装置に対するメディアキー等の鍵の暗号化処理について説明するツリー構成図である。

【図5】本発明の情報記録再生装置に対するメディアキー等の鍵の配布に使用されるキー更新ブロック（KRB）の例を示す図である。

【図6】情報記録再生装置におけるメディアキーのキー更新ブロック（KRB）を使用した配布例と復号処理例を示す図である。

【図7】本発明の情報記録再生装置におけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図である。

【図8】本発明の情報記録再生装置において適用可能なディスク固有キーの生成例を説明する図である。

【図9】本発明の情報記録再生装置において、適用可能なタイトル固有キーの生成処理例を示す図である。

【図10】本発明の情報記録再生装置において適用可能なブロック・キーの生成方法を説明する図である。

【図11】本発明の情報記録再生装置におけるメディアキーを使用したデータ再生処理時の復号処理を説明するブロック図である。

【図12】本発明の情報記録再生装置において使用されるキー更新ブロック（KRB）のフォーマット例を示す図である。

【図13】本発明の情報記録再生装置において使用されるキー更新ブロック（KRB）のタグの構成を説明する図である。

【図14】本発明の情報記録再生装置においてキー更新ブロック（KRB）を複数格納した記録媒体、および記

(22)

特開 2002-9759

41

録再生装置におけるキー更新ブロック (KRB) の更新処理を説明する図である。

【図15】本発明の情報記録再生装置におけるキー更新ブロック (KRB) の更新処理を説明するフロー図である。

【図16】本発明の情報記録再生装置においてキー更新ブロック (KRB) を複数格納した記録媒体、および最新のキー更新ブロック (KRB) を用いて取得されるキーによる暗号化を行なったコンテンツの格納処理を説明する図である。

【図17】本発明の情報記録再生装置におけるキー更新ブロック (KRB) を用いて取得されるキーによる暗号化、コンテンツの格納処理を説明するフロー図である。

【図18】本発明の情報記録再生装置におけるキー更新ブロック (KRB) を用いて取得されるキーによる復号、およびコンテンツの再生処理手順を説明するフロー図である。

【図19】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図20】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

【図21】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

【符号の説明】

100 記録再生装置
110 バス
120 入出力 I/F
130 MPEGコーデック
140 入出力 I/F
141 A/D, D/Aコンバータ
150 暗号処理手段
160 ROM
170 CPU

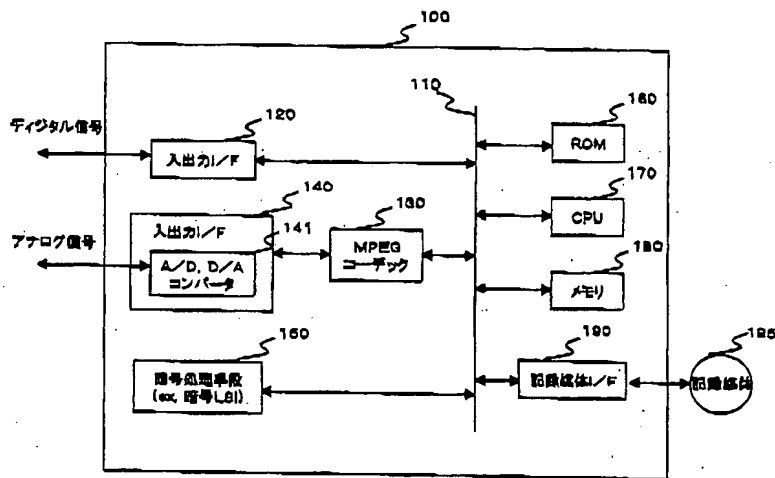
42

180 メモリ
190 ドライブ
195 記録媒体
700 記録再生装置
701 メディアキー
702 記録媒体
1201 バージョン
1202 デブス
1203 データポインタ
1204 タグポインタ
1205 署名ポインタ
1206 データ部
1207 タグ部
1208 署名
1410 記録再生装置
1411, 1412 キー更新ブロック (KRB)
1420 記録媒体
1421, 1422 キー更新ブロック (KRB)
1431, 1432 コンテンツ
16410 記録再生装置
1611 キー更新ブロック (KRB)
1620 記録媒体
1621, 1622 キー更新ブロック (KRB)
1631, 1632 コンテンツ
2101 バス
2102 CPU
2103 ROM
2104 RAM
2105 ハードディスク
2106 出力部
2107 入力部
2108 通信部
2109 ドライブ
2110 リムーバブル記録媒体
2111 入出力インタフェース

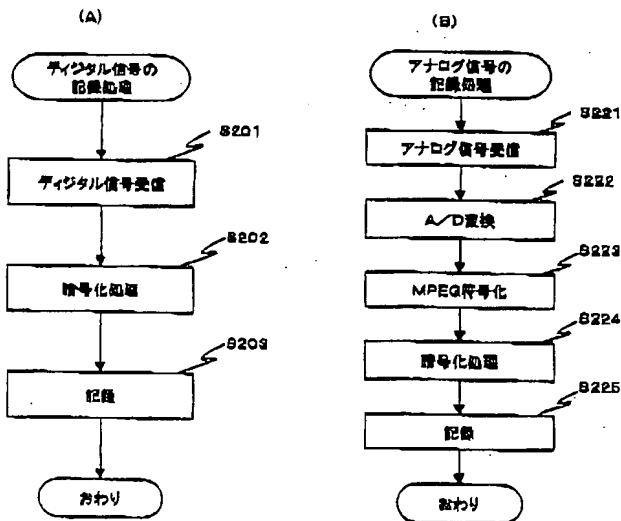
(23)

特開2002-9753

【図1】



【図2】



【図5】

(A) キー更新ブロック(KRB:Key Renewal Block) 例1

デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

世代(Generation):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K(t)000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K(t)0010, K(t)001)

(B) キー更新ブロック(KRB:Key Renewal Block) 例2

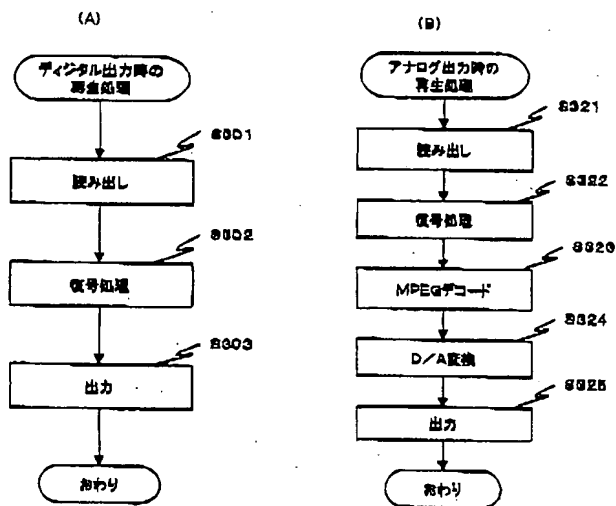
デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

世代(Generation):t	
インデックス	暗号化キー
000	Enc(K(t)000, K(t)R)
001	Enc(K(t)001, K(t)00)
0010	Enc(K(t)0010, K(t)001)

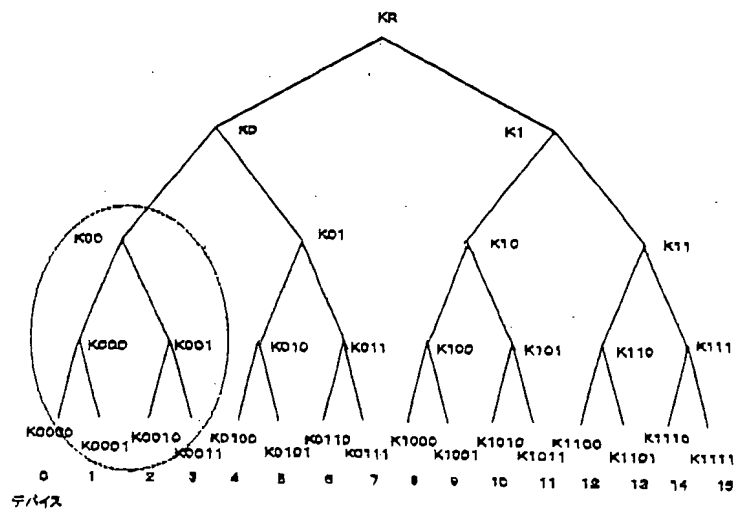
(24)

特開2002-9753

【図3】



【図4】



特開 2002-9758

記憶媒体

世代 (Generation) i	
インデックス	暗号化キー
000	Era(K000, K(i)00)
001	Era(K(v)001, K(i)00)
010	Era(K0010, K(v)001)
Era(K(i)00, K(v)media)	

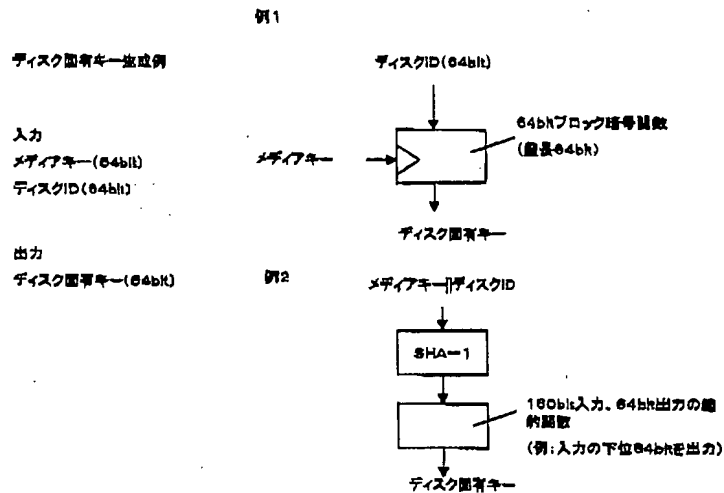
デバイス

[illegible]

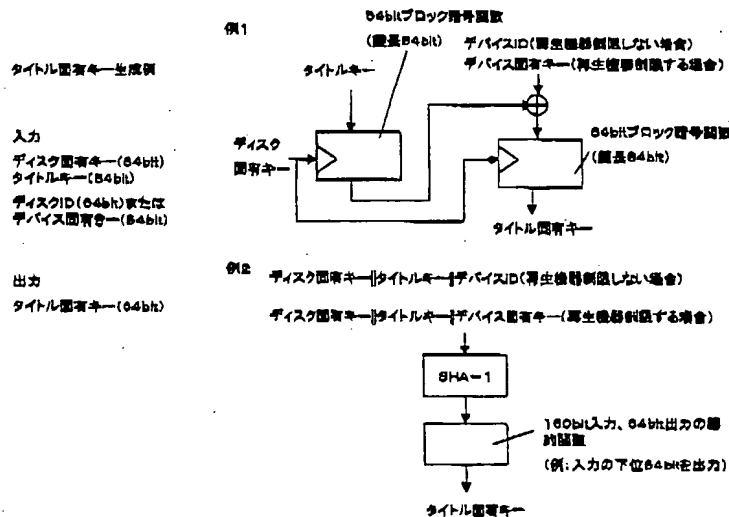
(28)

特開 2002-9753

【図 8】



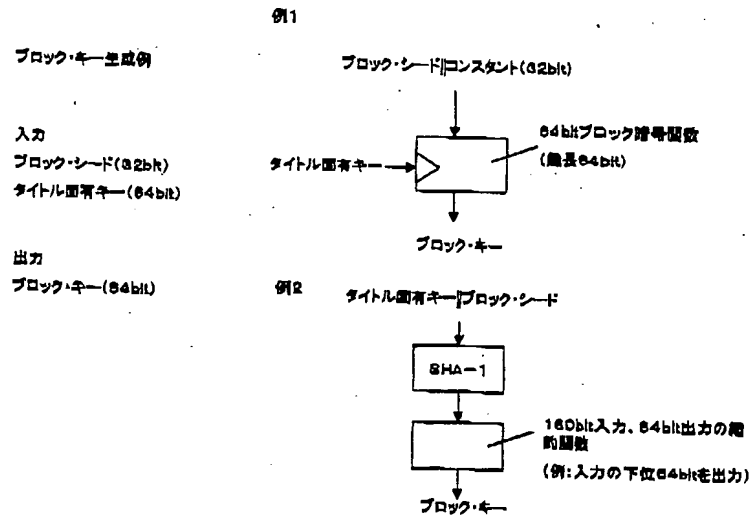
【図 9】



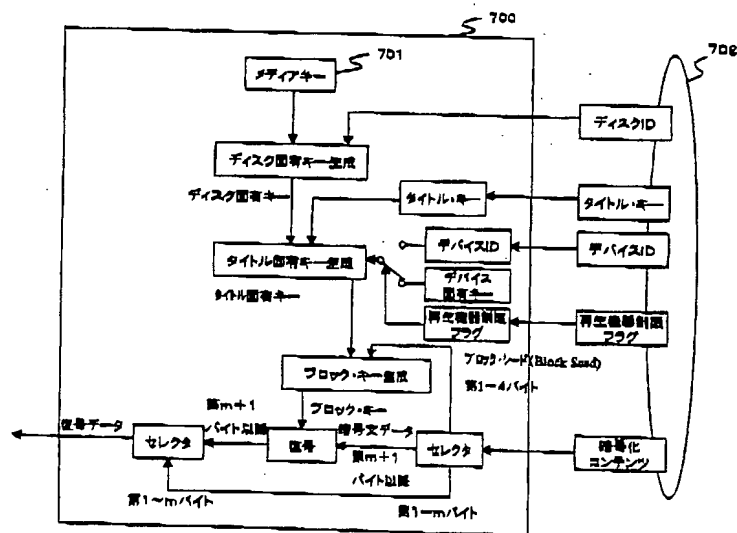
(27)

特開2002-9753

【図10】



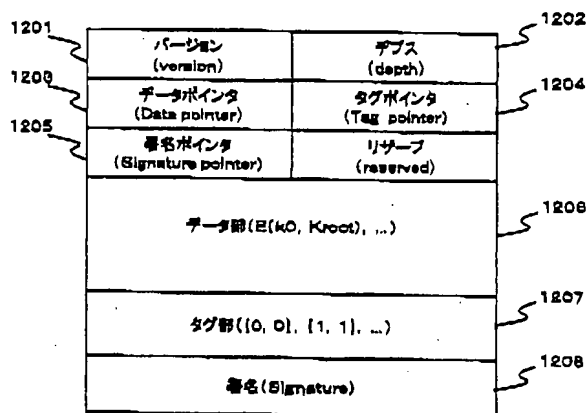
【図11】



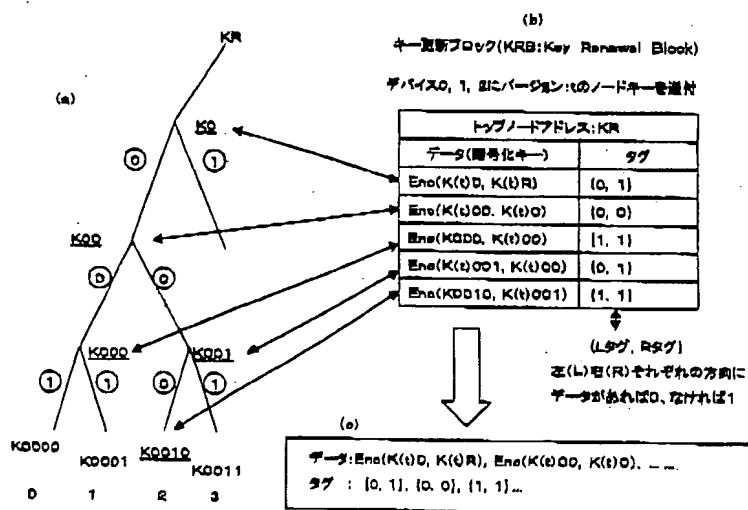
(28)

特開2002-9753

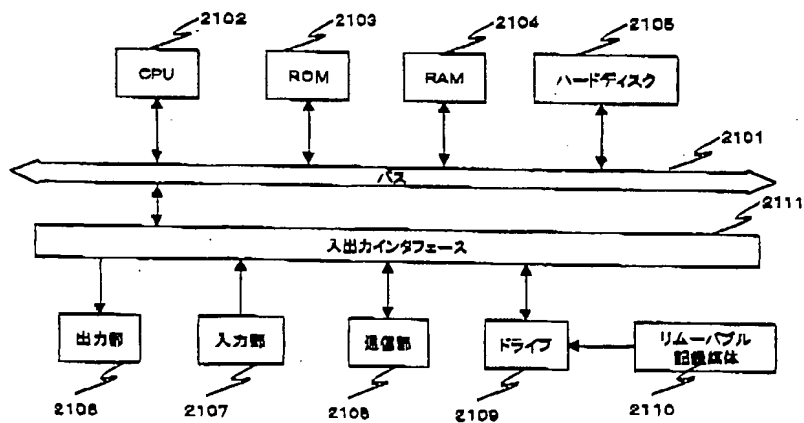
【図12】



【図13】



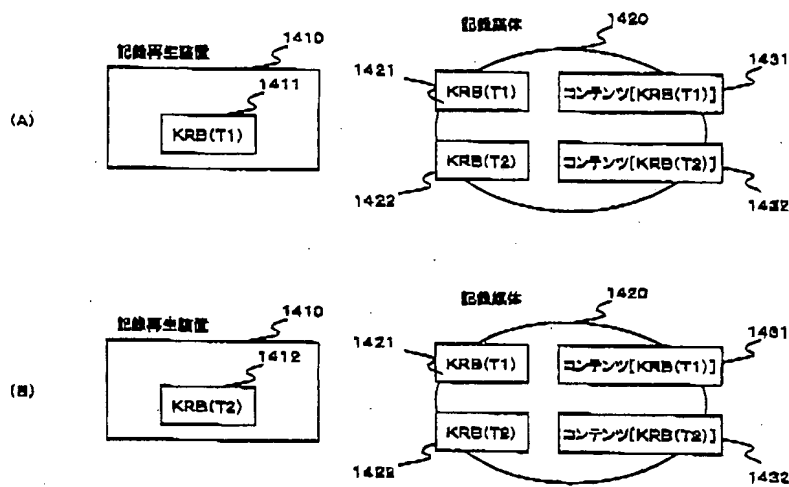
【図21】



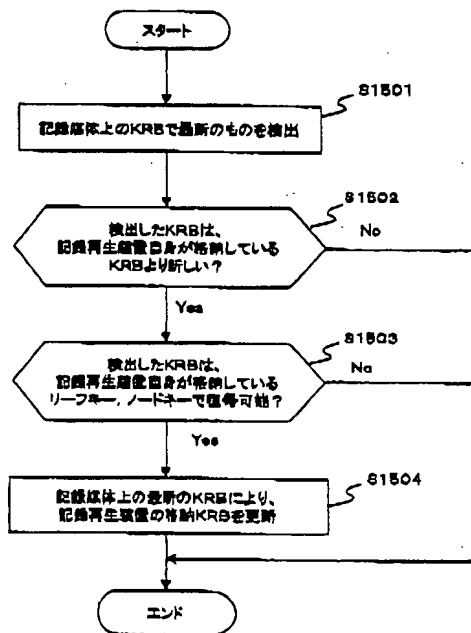
(29)

特開2002-9753

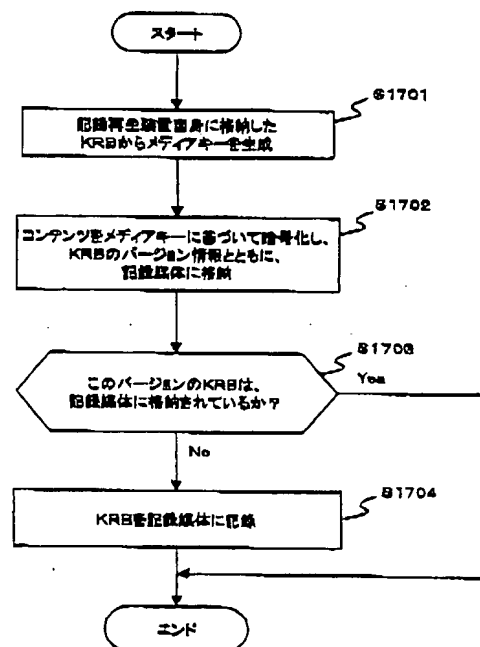
【図14】



【図15】



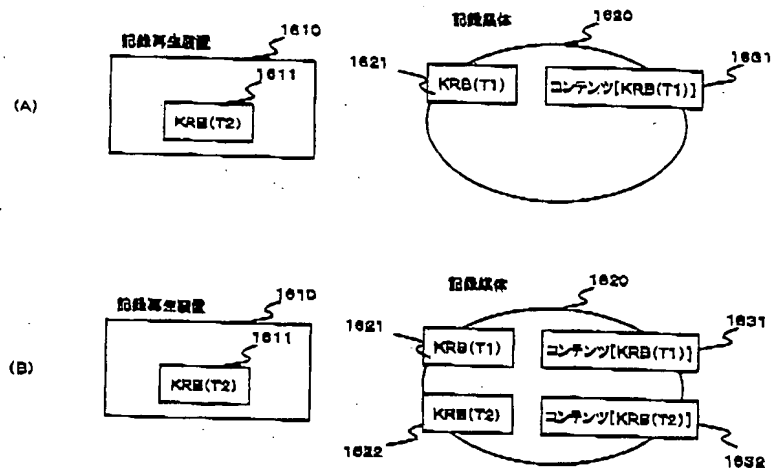
【図17】



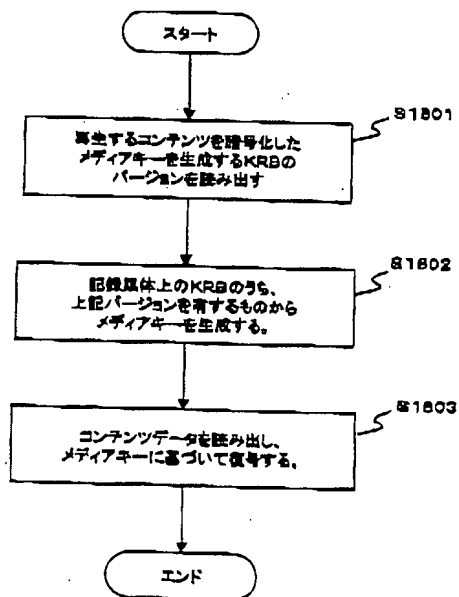
(30)

特開2002-9759

【図16】



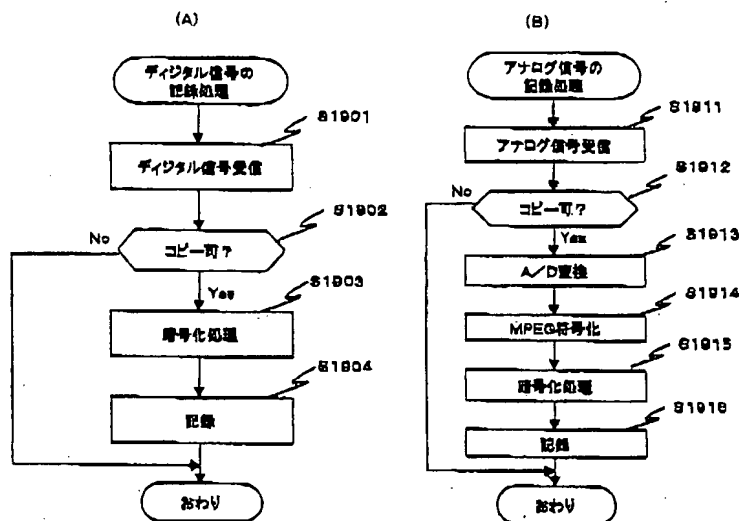
【図18】



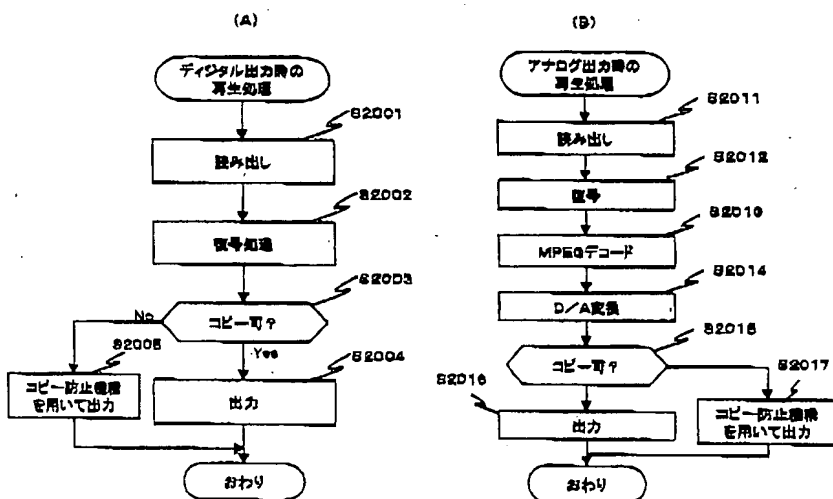
(31)

特開 2002-9758

【図19】



【図20】



フロントページの続き

(72)発明者 石黒 隆二

東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内

(72)発明者 光澤 敦

東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内

(72)発明者 大石 丈於

東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内

Fターム(参考) 5B017 AA07 BA07 CA16

5D044 AB05 AB07 BC04 BC08 CC06
CC09 DE47 DE50 DE59 EF05
FG18 GK12 HH13 HH15 HL08
5J104 AA01 AA16 EA01 EA07 EA17
EA24 NA02 PA14

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☐ FADED TEXT OR DRAWING

☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☒ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.